Build digital trust.
Simplify and scale your PKI.

EJBCA Enterprise® is a powerful certificate authority (CA) and PKI platform that is fast to deploy, scales on-demand, and supports any use case.

In a world where everything is connected and nothing is trusted, public key infrastructure (PKI) is the proven digital identity solution to enable secure, encrypted, and authenticated connections for every user, device, and workload. But PKI has always been hard, often due to complex and outdated systems that require in-depth expertise and cannot scale with modern use cases.

EJBCA Enterprise simplifies PKI operations and migrations from legacy CAs like Microsoft, providing an easy way to issue, manage and maintain digital certificates, even at massive scale. Built on open-source standards and an open-source platform, EJBCA is the most widely used and trusted CA software on the planet.

The platform comes pre-packaged with all the components required to run a robust & quantum-ready PKI, deploys wherever and however you need it, and scales on-demand, making it easy for teams to:

Simplify and consolidate PKI

Many internal PKI systems were built on older process and standards, resulting in overly complex and costly deployments. With EJBCA, you can run multiple PKI hierarchies on a single instance, centrally configure and govern certificate policies, and view detailed (and optionally signed) audit and transaction logs all in one place. Better yet, CAs and certificate templates can easily be configured, without requiring admins to be PKI experts.

Deploy fast — run anywhere

Every organization has unique business challenges, including security requirements, budgets and available IT resources. To meet these unique requirements and get up and running quickly, you can choose — or combine — any deployment model for your PKI, from a turnkey software appliance or hardware appliance with a built-in HSM, to a self-managed, containerized, or SaaS-delivered PKI deployed directly from the AWS or Azure marketplace. EJBCA can be deployed to meet your current needs and grow flexibly over time.

PKI For Any Use Case:

- Migrate from legacy Microsoft CAs to a modern multi-tenant, flexible enterprise PKI.
- Automate PKI deployment and certificate issuance for DevOps and microservices.
- Issue trusted identities for IoT devices and connected manufacturing environments.
- Enable secure government-issued and verified ePassports.
- Get quantum-ready with support for PQC and hybrid certificates.

Key Benefits:

- Protect critical systems and data and support zero-trust architecture with PKI-based identity.
- Enable developers and IT admins to move faster with sub-second certificate issuance.
- Meet stringent security and compliance requirements with a quantum-ready and trusted PKI.
- Reduce total cost of ownership (TCO) with pre-packaged appliances, containers, cloud, or SaaS PKI.
- Scale on-demand and issue millions of certificates under high-transaction loads.

Secure every device and workload

Containerization, DevOps, IoT devices and remote work all increase the number of machines and users that must be secured by an internal PKI. For this reason, EJBCA integrates with popular third-party applications and systems, extending your PKI to meet new use cases via support for widely used protocols and several pre-built plugins across different platforms and applications.

Supported technologies

Certificate formats and standards:

- RFC5280 compliant X.509 certificates and CRLs
- PKCS#10, CRMF and SPKAC certificate requests
- PKCS#12, JKS, PEM and PKCS#11 keystores
- EN 319 412 eIDAS compliant certificates
- C-ITS enrollment credentials as per ETSI and IEEE
- OCSP compliant with RFC6960 and RFC5019
- Payment Service Directive 2 (PSD2) ETSI TS 119495 Section 4
- ICAO 9303, EAC 1.11 and EAC 2.10 ePassport and eID
- RFC6962 compliant Certificate Transparency
- Hybrid PQC-ready certificates with 2 sets of keys

Protocols:

- ACME, EST, and SCEP enrollment/management protocols
- CMP and CMP 3GPP for 4G/5G mobile networks
- Microsoft Auto Enrollment
- Rest API
- Web Services

Hardware security modules (HSMs):

Thales Luna, Entrust nShield, Utimaco, Yubico, AWS CloudHSM, Azure Key Vault Managed HSM, Fortanix DSM, and other PKCS#11-compliant modules.

Cryptography:

RSA, ECDSA, and EdDSA keys, CNSA compliant. Dilithium and Falcon NIST PQC candidate algorithms.

Key Features:

One PKI platform, supporting multiple CAs, validation authorities (VAs), and registration authoritie (RAs) on a single instance.

High scalability for large-scale deployments with database-level clustering and HA configurations.

Deployment flexibility with PKI as a software or hardware appliance, container, cloud instance, or as a service (SaaS PKI).

Certificate lifecycle automation via native integration to Keyfactor Command or Keyfactor Control.

Easily integrates with Microsoft Intune, Active Directory (AD) and Azure AD, HashiCorp Vault, Kubernetes, and more.

Fast time to value with the ability to spin up CAs within minutes.

Trusted and compliant, including Common Criteria and NIAP certification, already deployed in WebTrust and ETSI/eIDAS compliant environments.

Quantum-ready and continuously updated with new features, backed by a full delivery and support team.

About Keyfactor

Keyfactor brings digital trust to the hyper-connected world with identity-first security for every machine and human. By simplifying PKI, automating certificate lifecycle management, and securing every device, workload, and thing, Keyfactor helps organizations move fast to establish digital trust at scale — and then maintain it. In a zero-trust world, every machine needs an identity and every identity must be managed.For more information, visit www.keyfactor.com

Get Started

Ready to modernize your PKI?

To get started with EJBCA, contact Keyfactor via email sales@keyfactor.com or phone +216-785-2946.